



# NOAA Mobile Device Management Policy

## Table of Contents

### [I. Purpose](#)

### [II. Scope](#)

### [III. Authority](#)

### [IV. Policy](#)

#### [\[01\] Acceptable Use](#)

#### [\[02\] Unacceptable Use](#)

#### [\[03\] Acceptable Mobile Applications on NOAA-provided Mobile Devices](#)

#### [\[04\] Purchase of Mobile Applications](#)

#### [\[05\] License Key Management](#)

#### [\[06\] Mobile Device Management](#)

#### [\[07\] International Travel](#)

### [V. Responsibilities](#)

### [VI. Management and Ownership](#)

### [VII. Intended Audience](#)

### [VIII. Implementation Date](#)

### [IX. Exceptions or Waivers](#)

### [X. Performance Objectives and Measurements](#)

### [XI. Definitions](#)

### [XII. Frequently Asked Questions \(FAQs\)](#)

### [XIII. Approval](#)

## **I. Purpose**

This memorandum establishes policy for the acquisition and use of mobile devices and applications, securing mobile data and Operating System (OS) configurations, and enforcing privacy mechanisms to safeguard NOAA authorized users.

## **II. Scope**

This policy applies to all mobile devices that access Government networks, data, and systems, except: laptops encrypted, maintained, and used in accordance with applicable NOAA policy and requirements, and non-NOAA-provided Mobile Devices that access government data only through the NOAA cloud sign-in at [google.com](http://google.com).

## **III. Authority**

Supersedes OCIO memorandum: NOAA Mobile Device Policy, February 3, 2012 and Transitioning from Blackberry Devices to iPhones dated April 19, 2012.

## IV. Policy

### [01] Acceptable Use

#### [A] Mobile users

**[01] Approved NOAA-provided Mobile Devices.** Devices approved for NOAA purchase may be found on the NOAA UMS intranet website (<https://sites.google.com/a/noaa.gov/noaa-ums/mobile>).

**[02] Use of Non-NOAA-provided mobile devices.** Non-NOAA-provided mobile devices are allowed to access government data only through the NOAA cloud sign-in at [google.com](https://google.com).

[a] Mobile users are prohibited to transmit, save, store, retain, or retrieve government data with Non-NOAA-provided mobile devices (including accessing email via IMAP) - except that Non-NOAA-provided mobile devices may access government data through the NOAA cloud sign-in at [google.com](https://google.com).

**[03]** Mobile users may transmit to another device or user, store, retain, or retrieve official NOAA data only on NOAA networks, government furnished devices, or NOAA-approved locations, or through the NOAA cloud sign-in at [google.com](https://google.com).

#### [B] Security

**[01]** NOAA and its component Line Offices, as well as NOAA employees and affiliates, have a requirement to protect NOAA's information assets in order to safeguard sensitive data including Personally and Business Identifiable Information, and other sensitive data.

**[a]** Users of NOAA-provided Mobile Devices must complete the annual NOAA IT Security Awareness training and agree to the NOAA Rules of Behavior for Mobile Devices and applicable mobile device policies prior to being granted a connection to NOAA systems and to continue to connect to NOAA systems each year.

**[b]** Any user of a NOAA-provided Mobile Device must report a lost or stolen device to a Line or Staff Office help desk as soon as practicable upon discovery that the device is no longer accounted for.

- The Line or Staff Office will coordinate with NOAA Computer Incident Response Team (N-CIRT) and other units consistent with established escalation processes.

**[c]** If a user suspects that unauthorized access has occurred to a NOAA-provided Mobile Device that has accessed government data they must report the incident as required by NOAA's IT Security incident handling policy.

**[02]** Unless otherwise specifically stated in this policy, Department of Commerce and NOAA IT security policies apply to mobile devices used to access NOAA systems and not to mobile devices that access government data through an NOAA cloud sign-in at [google.com](https://google.com).

## **[02] Unacceptable Use**

**[A]** Unacceptable or prohibited use of NOAA-provided Mobile Devices includes:

**[01]** Access or storage of classified data.

**[02]** Violation of any applicable federal, state, local law, regulation, or statute, or DOC/NOAA policy.

**[a]** By way of example, the device may not be used to access pornographic images, gambling, political fund raising, or personal business ventures.

**[b]** This applies to installing apps, the use of internet features, and mobile device use while driving.

**[03]** Unwarranted risks to privacy or IT security by violating mobile privacy or security policies, management system controls, or requirements.

**[04]** Installation of Unacceptable Applications, which are applications that are black-listed and posted on the NOAA UMS intranet website (<https://sites.google.com/a/noaa.gov/noaa-ums/mobile>).

**[05]** When cost is incurred by the government, unless specifically authorized and funded per section IV.[\[04\] Purchase of Mobile Applications](#).

**[06]** Compromise of any NOAA data, privacy, or security controls.

**[07]** Adverse effect on the performance of official duties by the employee or the employee's organization.

**[08]** Physical connections between mobile devices, both NOAA-provided and Non-NOAA-provided, with NOAA systems or computers.

**[a]** This includes the use of USB chargers connected to NOAA computers.

**[b]** Exceptions to this provision are permitted in cases where technical support is required.

**[B]** Unacceptable use, or failure to comply with any item in this policy may result in corrective actions, which may include, but are not limited to:

**[01]** Partial erasure, loss of function or operation, or having the device otherwise restricted, application removal, immediate wiping or disabling of the NOAA Mobile Device, without prior notice to the user.

**[02]** Applications (and any associated data), including those purchased with personal funds, may be deleted or erased, rendered inoperative, or be otherwise restricted.

**[03]** The termination of mobile device connection to NOAA systems.

**[04]** The loss of access to email.

**[05]** The confiscation of the mobile device, to include Non-NOAA-provided Mobile Device.

## **[03] Acceptable Mobile Applications on NOAA-provided Mobile Devices**

**[A]** All mobile applications used on NOAA-provided Mobile Devices that connect to the NOAA IT enterprise must meet the following requirements:

**[01]** Applications related to the performance of official duties.

**[02]** Complies with Section IV.[\[02\] Unacceptable Use](#).



#### **[04] Purchase of Mobile Applications**

**[A]** Applications for NOAA-provided iOS Mobile Devices may be purchased at government expense when approved by an employee's supervisor or customary approval process once a bona fide need has been established and documented.

**[01]** Any burden of showing that the application is necessary for a user's official duties, or otherwise justifying the expenditure of NOAA funds, falls on the employee making the request.

**[02]** Government purchasing of applications must follow DOC Purchase Card Program Commerce Acquisition Manual (CAM) 1313.301 (May 2012) [http://www.ago.noaa.gov/acquisition/docs/cam\\_1313.301\\_revised\\_may\\_2012.pdf](http://www.ago.noaa.gov/acquisition/docs/cam_1313.301_revised_may_2012.pdf).

**[B]** Currently, there is not a way to use government credit cards to purchase individual applications for Android devices. Therefore, purchase of Android applications using government funds is not authorized at this time.

**[C]** NOAA employees may purchase applications from approved sources (iTunes and Google Play) for use on a NOAA-provided Mobile Device with their own personal funds.

**[01]** To do so, users must create their own personal "Application Store" account and associate it with a personal credit card or payment mechanism and apply it to their NOAA Mobile Device.

**[02]** Users **may not** associate their official @NOAA.gov identity with their personal credit card.

**[03]** Purchasing an application with personal funds is at the sole discretion of the device holder, may not be considered as a requirement to perform your official duties, and is solely at the risk of the purchaser as these applications may be removed at any time deemed necessary under this policy.

**[04]** Any Terms of Service applicable to applications purchased with personal funds are between the user and the company. Personal accounts will not bind the government to contract.

**[05]** **NOAA will not reimburse device holders or users for any application or lost data under any circumstance.**

#### **[05] License Key Management**

**[A]** Subject to applicable NOAA and Department of Commerce procurement and administrative policies, applications installed on NOAA-provided Mobile Devices are considered expendable and consumable, unless the application is managed at an enterprise level.

**[01]** For enterprise-managed applications utilizing an external license key, the license key is considered non-expendable and must be retrieved and retained for future NOAA use.

**[02]** Provide to NOAA IT for recovery of any such key when a NOAA Mobile Device is excessed or otherwise disposed of once the device no longer needs access to NOAA systems or the device's owner is no longer associated with NOAA.

## **[06] Mobile Device Management**

**[A]** NOAA-provided Mobile Devices must be managed by a NOAA mobile device management system. The management system will do or enforce the following:

- [01]** All Government data on mobile devices that connect to NOAA systems must be encrypted to a level approved by the NOAA CIO.
- [02]** Install and maintain security- and/or management-related software on mobile devices. Such security/management software may change device configurations.
- [03]** Configure mobile devices to unlock using a device passcode.
- [04]** Perform an inventory of applications and data on the device.
- [05]** Monitor (and as necessary, control or limit) the installation or removal of applications.
- [06]** Remotely wipe (selective or full) mobile devices in the event of a security threat or violation of policy.
- [07]** Allow installation of mobile device applications available only from approved sources. In addition, control what specific applications or classes of applications may be restricted by NOAA or its Line Offices.

## **[07] International Travel**

**[A]** NOAA-Provided Mobile Device users must notify Line Office IT Security Officer or individual designated by the Line Office 10 business days prior to international travel, unless an exception is provided by the Department of Commerce (for more information, see FAQs).

**[B]** At a minimum, the Line Office IT Security Officer or individual designated by the Line Office must document:

- [01]** the dates of travel;
- [02]** countries of travel, including intermediate stopover;
- [03]** the nature and sensitivity of any data carried on the NOAA Mobile Device..

**[C]** The Line Office Security Officer or individual designated by the Line Office must:

- [01]** Instruct the user on the proper protection of the NOAA Mobile Device.
- [02]** Advise the user to review the Department of Commerce Office of Security (OSY) policies and to contact OSY.
- [03]** Ensure that any NOAA or Line Office or Staff Office defined sensitive data is appropriately encrypted at the file level (i.e., in addition to device-wide encryption).
- [04]** Disable NOAA-provided Mobile Device WiFi and Bluetooth connections for the period of travel, unless a waiver is granted by the Department of Commerce (for more information, see FAQs). Comply with existing Commerce Information Technology requirements.



## **V. Responsibilities**

[01] The NOAA CIO shall:

- [A] Retain the right to prohibit the use of any application on NOAA systems.
- [B] Manage the process of reviewing mobile devices and applications for compatibility with NOAA technical, security and privacy requirements and specifications.

[02] The Enterprise Collaboration Committee (ECC) shall:

- [A] Post prohibited applications (blacklist) (i.e. Unacceptable Applications) and reviewed and tested applications (whitelist), as well as procedural guidance on the evaluation process on the NOAA UMS intranet website (<https://sites.google.com/a/noaa.gov/noaa-ums/mobile>).
- [B] Review mobile devices and applications for risks to NOAA data and systems, as well as address any potential privacy concerns.

[03] NOAA OCIO Service Delivery Division shall:

- [A] Serve as, assign, or delegate a License Key Manager, who shall be responsible to manage non-expendable license keys.
- [B] Operate the Mobile Device Management system and asset inventory.
- [C] Maintain the pending and approved waivers or exceptions to this policy.
- [D] Manage this policy and serve as its point of contact.

[04] The Line Office IT Security Officer or other individual designated by the Line Office ACIO shall:

- [A] Support processes for the mobile user regarding lost or stolen NOAA-provided Mobile Devices, escalation, and coordination with N-CIRT.
- [B] Support the mobile user to comply with the [International Travel](#) Section of this policy.

## **VI. Management and Ownership**

The NOAA CIO owns this policy. The Service Delivery Division within OCIO manages this policy and serves as the point of contact.

## **VII. Intended Audience**

NOAA employees and affiliates.

## **VIII. Implementation Date**

This policy is effective immediately upon approval by the NOAA CIO or CIO Council.

## **IX. Exceptions or Waivers**

[01] The NOAA CIO or designee may grant exceptions or waivers, on a case by case basis, after:

1. Demonstration of sufficient business need and;
2. Completion of a risk assessment by security management.

[02] All waivers require approval from the Line Office ACIO and must be submitted to the NOAA CIO or designee.

## **X. Performance Objectives and Measurements**

100% of NOAA-provided Mobile Devices will be managed by a NOAA mobile device management system. (IV.[06] [Mobile Device Management](#))

## **XI. Definitions**


- **NOAA-provided Mobile Devices** - Government owned devices
- **Non-NOAA-provided Mobile Devices** - Personally owned devices
- **NOAA Employee** - NOAA Federal employees and commissioned corps employees.
- **NOAA Affiliate** - This includes employees of contractors, grantees, cooperative institutes, collaborators, universities, and other federal agencies.
- **Business Identifiable Information (BII)** - Information defined in the Freedom of Information Act (FOIA) as trade secrets or commercial or financial information, that is obtained from a person representing a business entity, and which is privileged and confidential (e.g., Title 13) and exempt from automatic release under FOIA.
- **Personally Identifiable Information (PII)** - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

## **XII. Frequently Asked Questions (FAQs)**

Mobile related FAQs may be found on the NOAA UMS intranet website (<https://sites.google.com/a/noaa.gov/noaa-ums/mobile>).

## **XIII. Approval**

This policy was approved on January 30, 2014 by the NOAA CIO.



Joseph F. Klimavicz, Chief Information Officer